Literature Review of Email Forensics

Pranali P. Hatole & Dr. Shobha K. Bawiskar
Government Institute of Forensic Science, Aurangabad

Abstract: Communication through email is widely used. Emails contain highly crucial information. Taking advantage of this cyber criminal takes unauthorized access and do unauthorized changes and use it any manner that can harm the person directly or indirectly. As the number of crimes are increasing in this area there is need arise to do investigation of emails, and hence Email forensic is important to study. Email will helps to gives important clue for further investigation.

Keywords: - E-mail forensics, Deleted Mail Recovery, Email forensic tools.

Introduction: -

E-mail forensics refers to the study of email details including: source and content of e-mail, in order to identify the actual sender and recipient of a message, date/time of transmission, detailed record of e-mail transaction as well as the intent of the sender. [1]

Past situation

Before 2000 crime rate in cyber cases was near to the ground. Most of the People were unaware of email and chats. Earlier period email was used for communication purpose in good faith not to harm others but now this scenario is changed.

Present situation

Today everyone is aware of email and use it commonly, because of this crimes using by email are mounting. Crime situations like homicide , Harassment, cyber stalking, cyber terrorism, cyber threatening , cyber defamation, fraud mails, phishing, email spamming ,email bombing etc. are seen widely happening now a day’s which is called as email crimes. Emails crimes are the emails that can be found as evidence.

As the report generated by National Crime Record Bureau (NCRB) of India cyber crime are continuously increasing. But because of ineffective investigation the percentage of solved cases are low. NCRB serve report 2015-16. As indicated in table 1 for Maharastra state [2]

<table>
<thead>
<tr>
<th>State</th>
<th>IT Act</th>
<th>IPC Section</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>2014</td>
<td>2015</td>
</tr>
<tr>
<td>Maharashtra</td>
<td>806</td>
<td>97</td>
</tr>
</tbody>
</table>

Table 1: NCRB 2015-16 report for Maharastra state

With reference to above details there is need to investigate emails and its relevant details. Hence existing literature study is done in detail.

Sobiya R. Khan et.al study shows that With growing email abuses investigators require efficient automated tools for fast e-mail analysis to help the forensic investigators gather evidence. Experiments on email classification like Decision Tree classifier have shown promising results. [3]

Techniques and Tools for Forensic Investigation of E-Mail

E-Mail Forensic Investigation Techniques:
1. Header Analysis
2. Bait Tactics
3. Server Investigation
4. Network Device Investigation
5. Software Embedded Identifiers
6. Sender Mailer Fingerprints

E-MAIL FORENSIC TOOLS:

1. EMailTracker Pro analyses the headers of an e-mail to detect the IP address of the machine that sent the message so that the sender can be tracked down. It can trace multiple e-mails at the same time and easily keep track of them.

2. EmailTracer It traces originating IP address and other details from e-mail header, generates detailed HTML report of email header analysis, finds the city level details of the sender, plots route traced by the mail and display the originating geographic location of the e-mail. Besides these, it has keyword searching facility on e-mail content including attachment for its classification.

3. Adcomplain This is used for reporting inappropriate commercial e-mail and Usenet postings, as well as chain letters and “make money fast” postings. It automatically
analyses the message, composes an abuse report, and mails the report to the offender's internet service provider by performing a valid header analysis.

4. Aid4Mail Forensic This is e-mail investigation software for forensic analysis, e-discovery, and litigation support. It is an e-mail migration and conversion tool, which supports various mail formats including Outlook (PST, MSG files), Windows Live Mail, Thunderbird, Eudora, and mbox. It can search mail by date, header content, and by message body content.

5. AbusePipe Analyses abuse complaint e-mails and determines which of ESP’s customers is sending spam based on the information in e-mailed Complaints. AbusePipe can be configured to automatically reply to people reporting abuse.

6. AccessData’s FTK is standard court-validated digital investigations platform computer forensics software delivering computer forensic analysis, decryption and password cracking within an intuitive and customizable interface. It has speed, analytics and enterprise-class scalability.

7. EnCase Forensic is computer forensic application that provides investigators the ability to image a drive and preserve it in a forensic manner using the EnCase evidence file format. It contains a full suite of analysis, bookmarking and reporting features. It supports Internet and e-mail investigation. The e-mail support includes for Outlook PSTs/OSTs, Outlook Express DBXs, Microsoft Exchange EDB Parser, Lotus Notes, AOL, Yahoo, Hotmail, Netscape Mail and MBOX archives.

8. FINALeMAIL can recover the e-mail database file and locates lost e-mails that do not have data location information associated with them. FINALeMAIL has the capability of restoring lost e-mails to their original state, recover full e-mail database files even when such files are attacked by viruses or damaged by accidental formatting. It can recover E-mail messages and attachments emptied from the ‘Deleted Items folder’ in Microsoft Outlook Express, Netscape Mail, and Eudora.

9. Sawmill-GroupWise is a GroupWise Post Office Agent log analyzer which can process log files in GroupWise Post Office Agent format, and generate dynamic statistics from them, analyzing and reporting events.

10. Forensics Investigation Toolkit (FIT) is content forensics toolkit to read and analyze the content of the Internet raw data in Packet CAPture (PCAP) format. FIT provides security administrative officers, auditors, fraud and forensics investigator as well as lawful enforcement officers the power to perform content analysis and reconstruction on pre-captured Internet raw data from wired or wireless networks. The other uniqueness of the FIT is that the imported raw data files can be immediately parsed and reconstructed.

11. Paraben (Network) E-mail Examiner It has comprehensive analysis features, easy bookmarking and reporting, advanced Boolean searching, searching within attachments, and full UNICODE language support. It can recover deleted e-mails from Outlook (PST), Thunderbird, etc.

M.Tariq Banday study shows that, this paper portrays e-mail actors, roles and their responsibilities. It illustrated logical e-mail architecture and underling various core components, modules and protocols used in the system. It presents the meta-data contained in e-mail message and various techniques used for e-mail forensics. The paper also introduces several software e-mail forensic tools that have functionalities to automatically analyze e-mail and produce reports providing diverse information about it. [4]

A Comparative Study of Email Forensic Tools.
Email Forensic Tools are MailXaminer, Add4Mail, Digital Forensic Framework, eMailTrackerPro, Paraben E-Mail Examiner Comparison done by following points:
1) Requirement of input files in the hard disk,
2) Search option
3) Information extracted or provided by the tool
4) Recovery capability
5) Email file format supported
6) Visualization support
7) Operating system (OS) supported
8) Extended device supported
9) Export format supported.

Vamshee Krishna Devendran et.al study shows that, they compare the tools based on nine criteria: input file in disk, search option, information provided, recovery capability, and format supported.
Visualization format supported, operating system supported, export format, and extended device support.
Analysis shows that among the five tools, Add4Mail can analyze emails stored both in hard disk (offline analysis) and on remote email servers (online analysis). In terms of the search option,
Add4Mail has the highest amount of capability to gather information than other tools. Among all tools, the information provided by Paraben Email Examiner covers not only email header and body, but also the attached file contents. The recovery capability of Add4Mail and Paraben Email Examiner look better than the other three tools since they can recover emails from delete folder. In terms of Email format support, Paraben Email Examiner supports most of the known email formats and 750 MIME content types. However, for visualization support, MailXaminer provides various options to end users. Most of the tools support Windows as the preferred OS, while only a few support Linux. The Digital Forensic Framework supports a rich set of output file format. Finally, very few tools (Add4Mail, Digital Forensic Framework) support extended devices such as USB memory stick. [5]

Towards an integrated email forensic analysis framework
Rachid Hadjiddj et.al study shows that - they developed an e-mail analysis framework to assist investigators gather clues and evidence in an investigation in which e-mail communication is relevant. The framework offers different functionalities ranging from e-mail storing, editing, searching, and querying to more advanced functionalities such as authorship attribution and e-mail account localization.[6]

Charalambs Elisavet et.al study shows that Email forensic tools used for email header analysis through a cybercrime use case. Tools are as follows- Aid4Mail, eMailTrackerPro, Paraben Email Examiner, EmailTracer, Adcomplain, AbusePipe, and FINALeMAIL are explained above.
1. Digital Forensics Framework (DFF): can analyze emails stored in hard disk while it can also perform some features like virtual machine disk reconstruction.
2. MailXaminer: It loads messages from the chosen email storage source and arranges them hierarchically for the purpose of evidence analysis and extraction. The programming of the application provides carving out of deleted evidence or evidence from damaged sources in cases of evidence spoliation
3. Internet Evidence Finder (IEF) by Magnet Forensics allows the definition of specific profiles for the recovery and detection of emails contained on physical drives. IEF is capable of recovering a range of files including PST, OST files as well as ‘mbox’ emails from which may extract emails, contacts, appointments, notes and tasks as well as any attachments
4. NUIX continues to lead the industry in breaking open data formats and forensic artifacts. It performs complex processes efficiently and consistently. Amongst its main features are email threading which groups email messages together so that the investigator can review them in context and make bulk decisions quickly.[1]

Gurpal Singh Chhabra et.al study shows that Email System, Security Protocols and Email Forensics Techniques are:-
1. Header Investigation
2. Server Investigation
3. Network and Network Device investigation
4. Investigation of Software Embedded details
5. Investigation and Discovery of Hidden Emails
6. Investigation of Anti Forensic Activity

Email Forensic Tools studied are:- MailXaminer, Aid4Mail, Digital Forensic Framework (DFF), EmailTrackerPro, Paraben EMX, EmailTracer.

MX Toolbox This software contain many tools like MX lookup, Blacklist, Diagnostics, Domain Health, Header Analyzer, DNS lookup and many more, each have some specific purpose. [7]

Conclusion:
Increasing numbers Threatening emails are received, confidential information also can be steal through email. Anyone can delete email after reading or use of important content from it because of which email forensics is needed. Based on detailed study various parameters like Header Analysis Email structure, E-mail header tracing, IP tracing, Bait Tactics, deleted email from trash are seen. Deleted mail can be recovered and restored from trash/ recycle bin from Yahoo, Rediff, Gmail and other email if accidently or intentionally deleted, but if mails are deleted from trash/ recycle bin the chances to recover them is very negligible. And hence it is seen that less work has been carried out on permanently deleted emails.

Future Work:-
Further research will be to see whether permanently deleted emails are recovered. While searching on this concern area following tools are found-MS-Outlook, Icarepro, RecoverMyEmail, Stellar Phoenix, Pareto DR, Recuva, EaseUs are used for experimental analysis which might resolve the problem of permanently deleted mails from the inbox and also from trash.

References
email header analysis through a cybercrime use case.”, Journal of Polish Safety and Reliability Association Summer Safety and Reliability Seminars, Volume 7, Number 1, 2016


[6] Rachid Hadjidj, Mourad Debbabi, Hakim Lounis, Farkhund Iqbal , Adam Szporer, Djamel Benredjem, “Towards an integrated e-mail forensic analysis framework”, Computer Security Laboratory, Concordia University, 1455 de Maisonneuve West, EV 7-642, Montreal, Quebec, Canada H3G 1M8